PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-237228
(43)Date of publication of application : 09.09.1997

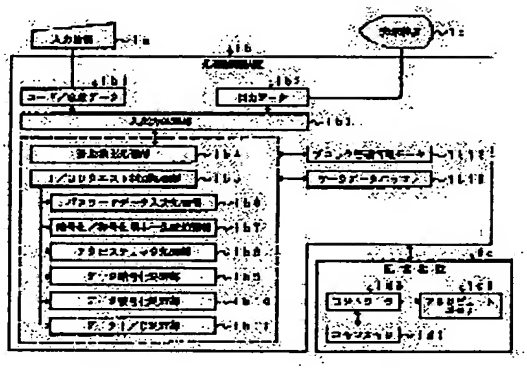
(51)Int.Cl. G06F 12/14
G06K 17/00
G09C 1/00
G09C 1/00
H04L 9/08
H04L 9/32

(21)Application number : 08-042913
(22)Date of filing : 29.02.1996

(71)Applicant : TOSHIBA CORP
(72)Inventor : MIURA YOSHIYUKI

(54) ACCESS CONTROL METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the security of a portable storage medium such as a PC card.
SOLUTION: At the time of formatting the PC card 1d, a user is allowed to input password data used for generating key data for ciphering/decoding for ciphering and decoding processings. Inputted password data is stored in the PC card 1d, key data for ciphering/decoding is generated by using the data and key data is announced to the user. When the user requests writing to the PC card 1d, it is confirmed whether password data exists in the PC card 1d or not. When it is stored, the user is allowed to input key data for ciphering/decoding and access right to the PC card 1d is checked. When they are matched as a result, data is ciphered by using key data and data is written in the PC card 1d.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－237228

(43)公開日　平成９年(1997)９月９日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｂ	
				３２０Ｃ	
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｅ	
Ｇ０９Ｃ　1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６３０Ｚ	
	６６０	7259－5Ｊ		６６０Ａ	

審査請求　未請求　請求項の数３　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平8－42913

(22)出願日　平成８年(1996)２月29日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　三浦　佳之
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

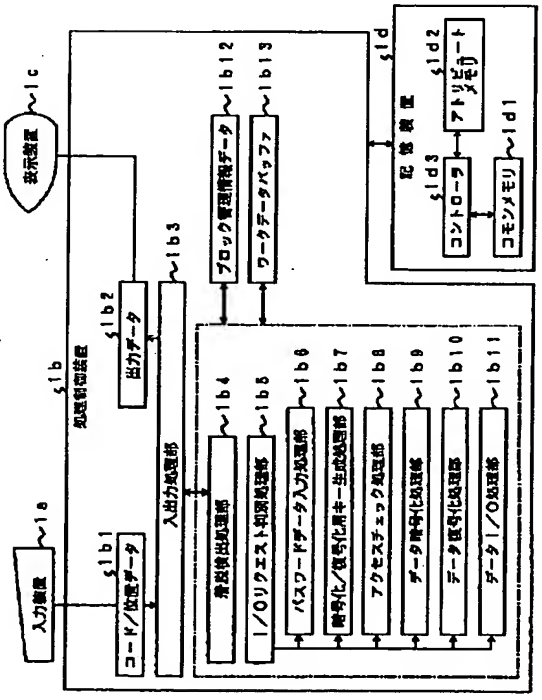
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　アクセス制御方法

(57)【要約】

【課題】ＰＣカードなどの可搬型記憶媒体に対するセキュリティー性の向上を図る。

【解決手段】ＰＣカード１ｄのフォーマット時は、その暗号化および復号化処理のための暗号化／復号化用キーデータを生成に用いるパスワードデータをユーザに入力させる。そして入力されたパスワードデータをＰＣカード１ｄ内に格納すると共に、そのデータを利用して暗号化／復号化用キーデータを生成し、そのキーデータをユーザにアナウンスする。ユーザがＰＣカード１ｄに対してライトリクエストした場合には、ＰＣカード１ｄ内にパスワードデータが存在するかを確認し、格納されている場合にユーザに暗号化／復号化用キーデータを入力させ、ＰＣカード１ｄへのアクセス権をチェックする。その結果一致していたならば、キーデータを使用してデータを暗号化した後、ＰＣカード１ｄ内にライトする。



1

【特許請求の範囲】

【請求項１】　可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、

ユーザからの入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納することによって、前記可搬型記憶媒体を初期設定し、

前記初期設定された可搬型記憶媒体が前記計算機システムに装着されたとき、あるいは前記装着された可搬型記憶媒体に対するデータ書き込み／読み出し要求が発行されたとき、前記可搬型記憶媒体から読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、

アクセス権を有すると判定したとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行うことを特徴とするアクセス制御方法。

【請求項２】　前記可搬型記憶媒体の着脱を検出し、前記可搬型記憶媒体が装着される度に前記アクセス権有無の判定処理を行うことを特徴とする請求項１記載のアクセス制御方法。

【請求項３】　ＰＣカードが取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、

ユーザからの入力パスワードに基づいて前記ＰＣカードに格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記ＰＣカードに格納することによって、前記ＰＣカードを暗号化カードとして初期設定し、

前記初期設定されたＰＣカードが前記計算機システムに装着されたとき、あるいは前記装着されたＰＣカードに対するデータ書き込み／読み出し要求が発行されたとき、前記ＰＣカードから読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記ＰＣカードに対するアクセス権の有無を判定し、

アクセス権を有すると判定したとき、前記ＰＣカードに対するデータ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行うことを特徴とするアクセス制御方法。

【発明の詳細な説明】

【０００１】

2

【発明の属する技術分野】この発明は、可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法に関する。

【０００２】

【従来の技術】従来、半導体メモリを内蔵したＰＣカードやフロッピーディスクなどの可搬型記憶媒体に対するデータ書き込みにおいては、書き込みデータを変形させることなく、そのままの状態で記憶媒体に格納するという方式が採用されており、データを書き込んだユーザ以外の他のユーザでも簡単にそのデータに対してアクセスすることができた。なお、この方式におけるデータセキュリティ方式としては、書き込み禁止や隠しファイルなど、それぞれのファイルまたはディレクトリ毎に属性情報を変更することにより、他のユーザからのアクセスを制限するというものが知られている。

【０００３】しかしながら、このようなセキュリティ方式を採用しても、ＰＣカード内やフロッピーディスクのデータ構成は誰でも容易に確認することができ、かつ、それらの属性も容易に変更することができるため、十分な秘匿性を得ることはできなかった。

【０００４】また、セキュリティを考慮したデータの格納方式としては、ＰＣカードなどの記憶媒体内にパスワードデータを格納し、アクセス時にパスワード入力を行うことにより、その記憶媒体に格納されているパスワードとの照合を行い、アクセス権をチェックした後、データライトおよびリードを行う方式が知られている。さらに、記憶するファイルまたはディレクトリ毎に暗号化処理を行うことにより他のユーザがアクセスしても有効なデータを取得することができないようにする方式もある。なお、この時に使用される暗号化用のキー（鍵）データは、それぞれファイルまたはディレクトリの属性情報として付加され、これを取得することにより、暗号化後のデータの復号化が実現される。

【０００５】しかし、これらのセキュリティー方式においては、ＰＣカードなどの記憶媒体内にパスワードまたは暗号化／復号化用キーデータ自体を格納しているため、Ｉ／Ｏアクセス時には解析できないものの、記憶媒体内のデータを解析することにより、それらの取得を行うことができ、その後容易にデータをアクセスすることができる。つまり、単一レベルでの秘匿しか行っていないため、容易にそれを解除することができ、これも秘匿性の低いものであった。

【０００６】

【発明が解決しようとする課題】上述したように、半導体メモリを内蔵したＰＣカードやフロッピーディスクなどの可搬型記憶媒体に対する従来のセキュリティ方式では、第三者が容易に属性を変更することができたり、パスワードや暗号化用のデータを解析し取得することができるため、個人単位で携帯する可搬型記憶媒体の個人情報を秘匿化するセキュリティ技術としては信頼性の低い

ものであった。

【０００７】この発明はこの様な点に鑑みてなされたものであり、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティー保持に適したアクセス制御方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】この発明は、可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、ユーザからの入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納することによって、前記可搬型記憶媒体を初期設定し、前記初期設定された可搬型記憶媒体が前記計算機システムに装着されたとき、あるいは前記装着された可搬型記憶媒体に対するデータ書き込み／読み出し要求が発行されたとき、前記可搬型記憶媒体から読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、アクセス権を有すると判定したとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行うことを特徴とする。

【０００９】このアクセス制御方法によれば、ＰＣカードやフロッピーディスクなどの可搬型記憶媒体を暗号カードとして使用するための初期設定時には、可搬型記憶媒体の暗号化および復号化処理のためのキーデータ生成に用いるパスワードの入力がユーザに促される。そしてユーザから入力されたパスワードを可搬型記憶媒体に格納すると共に、そのデータを利用してキーデータを生成し、そのキーデータをユーザに提示する。このようにして、可搬型記憶媒体には、キーデータ生成に使用したパスワードだけが格納され、キーデータはアクセス制御方法を実現するためのＩ／Ｏ制御システムとして使用されるソフトウェア内部で保持管理される。

【００１０】また、計算機システムに着脱自在に装着して使用されるという可搬型記憶媒体の特徴を考慮し、初期設定された可搬型記憶媒体が計算機システムに装着されたとき、あるいは装着された可搬型記憶媒体に対するデータ書き込み／読み出し要求が発行されたときに、アクセス権チェックが行われる。このアクセス権チェックでは、ユーザにパスワードではなく、キーデータを入力させ、それが、可搬型記憶媒体から読み出したパスワードから生成したキーデータと比較される。そして、アクセス権を有すると判定された場合には、データ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行う。

【００１１】したがって、データ暗号化および復号化処理を介したデータＩ／Ｏ制御が行われ、記憶媒体単位でのデータの秘匿を実現することができる。さらにその秘匿においては、記憶媒体には実際にデータ暗号化および復号化の際に使用されるキーデータを格納しておくのではなく、あくまでもそのキーデータを生成するための元となるパスワードのみが格納されているので、第三者が記憶媒体内のデータを単純に解析しただけでは秘匿を解くことはできない。よって、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティー保持に適したアクセス制御を実現できる。

【００１２】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図１には、この発明の一実施形態に係るアクセス制御方法が適用される計算機システムとそのシステムで実行されるプログラムの機能構成が示されている。ここでは、計算機システムに取り外し自在に装着可能な可搬型記憶媒体として、半導体メモリを搭載したＰＣカードを例にとって説明する。

【００１３】この計算機システムは、キーボードやマウスあるいはペンやトラックボールなどからなる入力装置１ａ、および表示装置１ｃを有する計算機本体を備えており、この計算機本体にはそれが電源オンの状態であってもＰＣカード１ｄの装着、取り外しを行うことができる。

【００１４】処理制御装置１ｂは、入力装置１ａより入力されたデータを判断することによりＰＣカード１ｄに対するＩ／Ｏリクエストを判別し、データ暗号化および復号化処理を介してＰＣカード１ｄへのデータＩ／Ｏ制御、また、これらの処理に応じて表示装置１ｃへの出力制御を行うものであり、その機能は計算機システム内のＣＰＵによって実行されるソフトウェアであるＰＣカードドライバを利用して実現されている。

【００１５】この処理制御装置１ｂは、入力装置１ａより入力されたコード／位置データ１ｂ１と表示装置１ｃに出力される文字データやグラフィックデータなどの出力データ１ｂ２を処理する入出力処理部１ｂ３と、計算機本体とＰＣカード１ｄとの着脱状態を検出する着脱検出処理部１ｂ４と、入出力処理部１ｂ３を介して処理された入力データよりＰＣカード１ｄに対するデータライトやデータリードなどのＩ／Ｏリクエストを判別するＩ／Ｏリクエスト判別処理部１ｂ５と、Ｉ／Ｏリクエスト判別処理部１ｂ５よりＰＣカード１ｄのフォーマットが要求された場合に、ＰＣカード１ｄへのデータライトおよびデータリードにおけるデータ暗号化および復号化用キーデータの生成に使用するパスワードデータの入力とＰＣカード１ｄへの格納を行うパスワードデータ入力処

理部１ｂ６と、パスワードデータ入力処理部１ｂ６より入力・格納されたパスワードデータよりデータ暗号化／復号化用キーデータを生成する暗号化／復号化用キー生成処理部１ｂ７と、ＰＣカード１ｄの装着時にデータ暗号化／復号化キーデータを使用してユーザのアクセス権をチェックするアクセスチェック処理部１ｂ８と、ＰＣカード１ｄへのデータライト時に対象データを暗号化するデータ暗号化処理部１ｂ９と、ＰＣカード１ｄへのデータリード時に対象データを復号化するデータ復号化処理部１ｂ１０と、ＰＣカード１ｄへのデータライトやデータリードなどのＩ／Ｏ処理を行うデータＩ／Ｏ処理部１ｂ１１と、データＩ／Ｏ処理部１ｂ１１にて使用するＰＣカードデータを管理するブロック管理情報データ１ｂ１２と、各処理部にて使用する変数やデータバッファとして利用するワークバッファ１ｂ１３より構成される。

【００１６】また、ＰＣカード１ｄは、計算機本体からのデータＩ／Ｏコントロール処理信号に応じてコモンメモリ１ｄ１やアトリビュートメモリ１ｄ２へのデータリード／ライト制御を行うコントローラ１ｄ３と、コントローラ１ｄ３を介して計算機本体から送信されるデータを格納するコモンメモリ１ｄ１と、ＰＣカード１ｄの属性情報が格納されているアトリビュートメモリ１ｄ２より構成される。なお、これらのメモリは、フラッシュＥＥＲＰＯＭなどの不揮発性メモリを使用して構成される。

【００１７】図２は、ブロック管理情報データ１ｂ１２の構成図である。ＰＣカードへ１ｄのデータライトは、ハードディスク装置やフロッピィディスク装置同様、ブロック（セクタ）単位でのデータＩ／Ｏ制御を行うため、ＰＣカード内の総ブロック数データ２ａと、使用不能となった不要ブロックを管理するための不良ブロック数データ２ｂと、不良ブロックとなったブロックＮｏ．１～Ｎデータ２ｃと、不良になったブロックの代替先であるスペアブロックのスペアブロック数データ２ｄと、スペアブロックの代替ブロック数であるスペアブロック登録数データ２ｅと、スペアブロックＮｏ．１～Ｎデータ２ｆを備えて構成する。

【００１８】図３は、アトリビュートメモリ１ｄ２の構成図である。アトリビュートメモリには、ＰＣカードサイズ３ａと、スペアブロック数３ｂと、製造メーカ名３ｃと、リリースバージョン３ｄと、パスワードデータ３ｄなどのカード属性情報が格納されている。

【００１９】以降、ＰＣカードドライバを利用して実行されるＰＣカード１ｄに対するアクセス制御の手順を説明する。まず、アクセス制御処理の基本的な流れについて説明する。

【００２０】ＰＣカード１ｄのフォーマット時（暗号化カードとしての初期設定時）には、ＰＣカード１ｄに格納されるデータに対して暗号化処理を使用するかをユーザに選択させ、使用する場合に、その暗号化および復号化処理のための暗号化／復号化用キーデータを生成に用いるパスワードデータをユーザに入力させる。そして入力されたパスワードデータをＰＣカード１ｄ内に格納すると共に、そのデータを利用して暗号化／復号化用キーデータを生成し、そのキーデータをユーザにアナウンスする。

【００２１】ユーザがＰＣカード１ｄに対してライトリクエストした場合には、ＰＣカード１ｄ内にパスワードデータが存在するかを確認し、格納されている場合にユーザに暗号化／復号化用キーデータを入力させ、ＰＣカード１ｄへのアクセス権をチェックする。その結果一致していたならば、キーデータを使用してデータを暗号化した後、ＰＣカード１ｄ内にライトする。

【００２２】また、ユーザがＰＣカード１ｄに対してリードリクエストした場合には、ＰＣカード１ｄ内にパスワードデータが存在するかを確認し、格納されている場合にユーザに暗号化／復号化用キーデータを入力させ、ＰＣカード１ｄへのアクセス権をチェックする。その結果一致していたならば、キーデータを使用してデータを復号化した後、リードリクエストコマンドにそのデータを送信する。

【００２３】具体的には、以下のステップを利用してアクセス制御が行われる。

１）計算機本体の入力装置１ａおよび表示装置１ｃまたは音声出力機構を介して、ユーザへの入力や確認を促す入出力ステップ。

【００２４】２）ＰＣカード１ｄと計算機本体との着脱状態を検出する着脱検出ステップ。３）ＰＣカード１ｄに対するＩ／Ｏ要求内容を取得しその内容を判断するＩ／Ｏリクエスト判別ステップ。

【００２５】４）Ｉ／Ｏリクエスト判別ステップにより判別されたＩ／Ｏ内容がフォーマットである場合に、入出力ステップによりＰＣカード１ｄに対してデータの暗号化を設定するか否かの選択を促し、選択結果を判断し暗号化設定が選択されたと判断した場合に、ＰＣカード１ｄ内のデータを暗号化または復号化するために使用する暗号化／復号化キーの生成に使用するパスワードデータの入力を促し、入力されたパスワードデータを取得した後、ＰＣカード１ｄ内に格納（記憶）するパスワードデータ入力ステップ。

【００２６】５）ＰＣカードフォーマット時にＰＣカード１ｄ内に格納されたパスワードデータを取得し、そのデータを元にデータ暗号化／復号化に使用されるキーデータを生成する暗号化／復号化用キー生成ステップ。

【００２７】６）暗号化／復号化用キー生成ステップにより生成された暗号化／復号化用キーデータをユーザにアナウンスするアナウンスステップ。

７）ＰＣカード１ｄに対するアクセス権を判断するために、ＰＣカード１ｄ内にパスワードデータが存在するか

否かを判別し、入出力ステップにより暗号化／復号化用キーデータ入力を促す表示を行い、これにより入力されたデータと、ＰＣカード１ｄ内に格納されたパスワードデータから生成したキーデータとを比較しアクセス権の合否を判定するアクセスチェックステップ。

【００２８】８）着脱検出ステップによりＰＣカード１ｄが計算機本体に装着されたと判断され、アクセスチェックステップによりアクセス権を取得し、Ｉ／Ｏリクエスト判別ステップによりＰＣカード１ｄに対してデータライトリクエストが判別された場合に、アクセスチェックステップにて生成されたキーデータを使用して対象となるライトデータを暗号化した後、ＰＣカード１ｄ内に格納するデータ暗号化ステップ。

【００２９】９）着脱検出ステップによりＰＣカード１ｄが計算機本体に装着されたと判断され、アクセスチェックステップによりアクセス権を取得し、Ｉ／Ｏリクエスト判別ステップによりＰＣカード１ｄに対してデータリードリクエストが判別された場合に、アクセスチェックステップにて生成されたキーデータを使用して対象となるＰＣカード１ｄ内のデータであるリードデータを復号化した後、復号データをリクエスト側に渡すデータ復号化ステップ。

【００３０】次に、図４のフローチャートを参照して、ＰＣカード１ｄへのアクセス制御処理の流れを具体的に説明する。このアクセス制御処理は、前述したように、計算機本体のメインメモリに常駐するＰＣカードドライバによって実現されており、計算機本体を起動した際にＰＣカード１ｄの認識処理などが行われ、そのＰＣカード１ｄに対するＩ／Ｏリクエスト待ちの状態になる。

【００３１】計算機本体の入力装置１ａよりＰＣカード１ｄに対するＰＣカードフォーマットやデータライトあるいはデータリードなどのＩ／Ｏリクエストコマンドが実行された場合、ＰＣカードドライバは、コード／位置データ１ｂ１および入出力処理部１ｂ３を介して、Ｉ／Ｏリクエストを受け取る（ステップ４ａ）。

【００３２】そして、ＰＣカード１ｄが計算機本体に装着されているかを着脱検出処理部１ｂ４にて判別する（ステップ４ｃ）。その結果、ＰＣカード１ｄが装着されていない場合には、Ｉ／Ｏリクエストコマンドプログラムが保持しているステータスデータ内にエラーステータスをセットした後、Ｉ／Ｏコマンドプログラムに戻る（ステップ４ｄ、４ｅ）。

【００３３】なお、本実施形態のＰＣカードドライバでは、計算機本体の起動開始から終了時までのＰＣカードの装着状態を計算機本体を介してＰＣカードが割り当てられたドライブごとに管理しており、それを着脱フラグとして保持している。

【００３４】ＰＣカード１ｄが正常に装着されていた場合には、Ｉ／Ｏリクエスト判別処理部１ｂ５により受け取ったＩ／Ｏリクエストの内容を解析し、データＩ／Ｏ

処理部１ｂ１１にてＩ／Ｏリクエストの内容に応じた処理を行う（ステップ４ｆ～４ｉ’）。

【００３５】ここで、主なデータＩ／Ｏリクエストに対応する処理の流れについて説明する。

（ＰＣカードフォーマット処理）Ｉ／Ｏリクエスト判別処理部１ｂ５により、受け取ったＩ／Ｏリクエストがフォーマットの場合、本ＰＣカードドライバは、入出力処理部１ｂ３により計算機本体の表示装置１ｃを介して、ユーザに対して、データ暗号化および復号化処理機能付きのＰＣカードとしてフォーマットを行うかについての選択を促すために、選択用画面を表示する（ステップ４ｆ、４ｇ）。

【００３６】その結果、ユーザがデータ暗号化および復号化機能付きフォーマットを選択した場合には、パスワードデータ入力処理部１ｂ６より、データ暗号化／復号化用のキー（鍵）データの生成に使用するパスワードデータの入力をユーザに促す画面を表示する（ステップ４ｈ、４ｉ）。

【００３７】そして、入力されたパスワードを元に、暗号化／復号化用キー生成処理部１ｂ７によりデータ暗号化および復号化処理で使用する暗号化／復号化キーデータを生成し、表示装置１ｃに表示してユーザにアナウンスする（ステップ４ｊ）。そして、ユーザが入力したパスワードデータをＰＣカード１ｄ内のアトリビュートメモリ１ｄ２内にコントローラ１ｄ３を介して格納するとともに、ブロック管理情報データ１ｂ１２など参照してＰＣカード１ｄ内のメモリをフォーマットする（ステップ４ｋ）。そしてフォーマットコマンドプログラム内のステータスデータ内にステータス値をセットし、コマンドプログラムに処理を戻す（ステップ４ｌ）。

【００３８】なお、データ暗号化および復号化付きフォーマットの確認ステップ（ステップ４ｇ）にて、ユーザがデータ暗号化および復号化処理なしのフォーマットを選択した場合には、通常のフォーマット処理を行いステータス値をセットした後、コマンドプログラムに処理を戻す。

【００３９】（データライト処理）Ｉ／Ｏリクエスト判別処理部１ｂ５により、受け取ったＩ／Ｏリクエストがデータライトの場合、本ＰＣカードドライバは、ＰＣカード１ｄが挿入されているドライブに対応する脱着フラグの状態と、ＰＣカード１ｄ内のアトリビュートメモリ１ｄ２をチェックする（ステップ４ｎ）。その結果、データ暗号化用にフォーマットされたＰＣカード１ｄが、アクセスチェック処理部１ｂ８を介してアクセス権を取得していない場合（例えば、アクセスチェックが一度も行われてない、またはアクセスチェック後にカードの着脱が行われている）は、アクセスチェック処理部１ｂ８により表示装置１ｃを介して、画面上にデータ暗号化および復号化用キーデータの入力画面を表示し、ユーザにデータ暗号化／復号化用キーデータの入力を促す（ステ

ップ４ｏ、４ｐ）。

【００４０】そして、ユーザが入力したデータ暗号化／復号化用キーデータが有効かを判断するために、ＰＣカード１ｄ内のアトリビュートメモリ１ｄ２内に格納されているパスワードデータよりデータ暗号化／復号化用キーデータを生成して比較を行う。比較の結果、キーデータが一致する場合は、そのキーデータを使用して、対象となるライトデータを暗号化処理部１ｂ９により暗号化した後、コントローラ１ｄ３およびアトリビュートメモリ１ｄ２内データを介して、コモンメモリ１ｄ１に格納する（ステップ４ｔ、４ｖ）。そして、ステータス値をセットした後、ライトコマンドに処理を戻す（ステップ４ｗ）。

【００４１】なお、データ暗号化／復号化用キーデータの比較の結果、不一致の場合には、表示装置１ｃの画面上にエラーメッセージを表示し、エラーステータス値をセットしてライトコマンドに処理を戻す（ステップ４ｑ～４ｓ）。

【００４２】また、アクセスチェック処理部１ｂ８にてアクセス権を取得してからＰＣカード１ｄが脱着されていない場合には、アクセスチェックステップを行う必要がないと見なし、アクセスチェックなしで、データを暗号化する。また、ＰＣカード１ｄのアトリビュートメモリ内にパスワードデータが存在しない場合には、アクセスチェックおよびデータ暗号化ステップを行わずに、通常通りデータライトを行う。

【００４３】（データリード処理）Ｉ／Ｏリクエスト判別処理部１ｂ５により、受け取ったＩ／Ｏリクエストがデータリードの場合の処理は、上記データライト処理の流れとほぼ同様な処理が行われ、データ暗号化ステップの代わり、その部分でデータ復号化ステップが行われる。

【００４４】すなわち、Ｉ／Ｏリクエスト判別処理部１ｂ５により、受け取ったＩ／Ｏリクエストがデータリードの場合、本ＰＣカードドライバは、ＰＣカード１ｄが挿入されているドライブに対応する脱着フラグの状態と、ＰＣカード１ｄ内のアトリビュートメモリ１ｄ２をチェックする（ステップ４ｙ）。その結果、データ暗号化用にフォーマットされたＰＣカード１ｄが、アクセスチェック処理部１ｂ８を介してアクセス権を取得していない場合（例えば、アクセスチェックが一度も行われてない、またはアクセスチェック後にカードの着脱が行われている）は、アクセスチェック処理部１ｂ８により表示装置１ｃを介して、画面上にデータ暗号化および復号化用キーデータの入力画面を表示し、ユーザにデータ暗号化／復号化用キーデータの入力を促す（ステップ４ｚ、４ａ’）。

【００４５】そして、ユーザが入力したデータ暗号化／復号化用キーデータが有効かを判断するために、ＰＣカード１ｄ内のアトリビュートメモリ１ｄ２内に格納されているパスワードデータよりデータ暗号化／復号化用キーデータを生成して比較を行う。比較の結果、キーデータが一致する場合は、そのキーデータを使用して、対象となる暗号化データを読み出して復号化した後、それを要求元に渡す（ステップ４ｅ’、４ｇ’）。そして、ステータス値をセットした後、ライトコマンドに処理を戻す（ステップ４ｈ’）。

【００４６】なお、データ暗号化／復号化用キーデータの比較の結果、不一致の場合には、表示装置１ｃの画面上にエラーメッセージを表示し、エラーステータス値をセットしてリードコマンドに処理を戻す（ステップ４ｂ’～４ｄ’）。また、アクセスチェック処理部１ｂ８にてアクセス権を取得してからＰＣカード１ｄが脱着されていない場合には、アクセスチェックステップを行う必要がないと見なし、アクセスチェックなしで、データを復号化する。また、ＰＣカード１ｄのアトリビュートメモリ内にパスワードデータが存在しない場合には、アクセスチェックおよびデータ復号化ステップを行わずに、通常通りデータリードを行う。

【００４７】以上の手順によれば、実際にデータの暗号化および復号化に使用するキーデータでなく、そのキーデータを生成するためにユーザに入力させたパスワードデータをＰＣカード１ｄ内に格納することにより、キーデータはカード内部に物理的に存在しなくなり、第三者がＰＣカード内データを解析することによりパスワードデータを取得することができたとしても、データを復号することは困難となる。よって、データの秘匿を保持することができる。

【００４８】また、計算機システムに着脱自在に装着して使用されるというＰＣカード１ｄの特徴を考慮し、暗号化カードとして初期設定されたＰＣカード１ｄに対するアクセスチェックが行われていない場合、またはアクセスチェック後にカードの着脱が行われている場合に、データ書き込み／読み出し要求に応答して、アクセス権チェックが行われる。このアクセス権チェックでは、ユーザにパスワードではなく、キーデータを入力させ、それが、可搬型記憶媒体から読み出したパスワードから生成したキーデータと比較される。そして、アクセス権を有すると判定された場合には、データ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行う。したがって、ＰＣカード１ｄの着脱が行われても、アクセス権を正しく判定することができる。

【００４９】このように、データ暗号化および復号化処理を介したデータＩ／Ｏ制御を行うことにより、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つＰＣカード１４などの可搬型記憶媒体のセキュリティー保持に適したアクセス制御を実現できる。

【００５０】なお、図４では、データライト／リードの

11

度にアクセスチェックを行うか否かを判定したが、暗号化されたＰＣカード１ｄが新たに装着されたときに実行するカード認識処理にてアクセスチェックを行えば、その後、そのカード着脱が行われるまでは、アクセスチェックを省略しても良い。

【００５１】この場合のカード認識処理およびＩ／Ｏ処理の手順をそれぞれ図５、図６に示す。ＰＣカード１ｄが計算機本体に装着される度、ＰＣカードドライは、図５の手順でカード認識処理を行う。すなわち、その装着されたＰＣカード１ｄにパスワードが格納されているか否かに応じて、それが暗号化カードであるか否かを調べる（ステップＳ１１）。暗号化カードでない場合には、それを通常の非暗号化カードとして認識する（ステップＳ１４）。

【００５２】パスワードが格納されている暗号化カードである場合には、ＰＣカードドライは、ユーザにデータ暗号化／復号化用キーデータの入力を促す。そして、ユーザが入力したデータ暗号化／復号化用キーデータが有効かを判断するために、ＰＣカード１ｄ内のアトリビュートメモリ１ｄ２内に格納されているパスワードデータよりデータ暗号化／復号化用キーデータを生成して比較を行う（ステップＳ１２）。比較の結果、一致していれば正当なそのカードが正当な暗号化カードであると認識され（ステップＳ１３，Ｓ１５）、不一致であれば、エラー発生の通知が行われる（ステップＳ１６）。

【００５３】このような認識処理が行われたカードを着脱することなく使用する場合においては、データライトリクエストおよびデータリクエストに応じて図６の処理が行われる。

【００５４】すなわち、Ｉ／Ｏリクエスト判別処理部１ｂ５により、受け取ったＩ／Ｏリクエストがデータライトの場合（ステップＳ２１）、本ＰＣカードドライバは、ライト対象のカードが暗号化カードとして認識されたものであるか否かを調べる（ステップＳ２２）。暗号化カードとして認識されている場合には、フォーマット処理ですでに生成されているキーデータを利用して、ライトデータを暗号化した後にカードに書き込む（ステップＳ２３，Ｓ２４）。暗号化カードでない場合には、暗号化を行わずに、即座にデータ書き込みを行う（ステップＳ２４）。

【００５５】同様に、受け取ったＩ／Ｏリクエストがデータリードの場合は（ステップＳ２５）、本ＰＣカードドライバは、リード対象のカードが暗号化カードとして認識されたものであるか否かを調べる（ステップＳ２６）。暗号化カードとして認識されている場合には、フォーマット処理ですでに生成されているキーデータを利用して、記憶データを復号化した後に読み出す（ステップＳ２７，Ｓ２８）。暗号化カードでない場合には、復号化を行わずに、即座にデータを読み出す（ステップＳ２８）。

12

【００５６】なお、この発明は上述した実施形態に限定されるものではなく、ユーザにデータ暗号化および復号化機能付きＰＣカードフォーマットの設定についての選択や、パスワードあるいは暗号化／復号化キーデータを入力を促す際のアナウンス手段として、音声出力装置による音声でのアナウンスを用いてもよい。また、データの暗号化および復号化処理として、本実施形態では具体的にその方式について述べなかったが、この方式については秘密鍵暗号方式や公開鍵暗号方式であっても良い。また、アクセス権をチェックする際に、キーデータが一致するまでのリトライ回数を複数回設けても良い。さらに、ＰＣカード内に格納されるパスワードデータについて、本実施形態では、ＰＣカード内のアトリビュートメモリ内に格納するように述べたが、コモンメモリ内であっても良い。

【００５７】

【発明の効果】以上説明したように、本発明によれば、ＰＣカードなどの可搬型記憶媒体単位でのデータの秘匿を実現することができる。さらにその秘匿においては、記憶媒体内には実際にデータ暗号化および復号化の際に使用されるキー（鍵）データを格納しておくのではなく、あくまでもそのキーデータを生成するための元となるパスワードデータのみを格納しておくことにより、第三者が記憶媒体を解析しただけでは秘匿を解くことができない。よって、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティー保持に適したアクセス制御を実現できる。

【図面の簡単な説明】

【図１】この発明の一実施形態に係るアクセス制御方法が適用される計算機システムの構成を示すブロック図。

【図２】同実施形態の計算機システムで使用されるＰＣカードのデータ管理構造を説明するための図。

【図３】同実施形態の計算機システムで使用されるＰＣカードのアトリビュートメモリのデータ構造を説明するための図。

【図４】同実施形態の計算機システムにおけるアクセス制御処理の流れを説明するフローチャート。

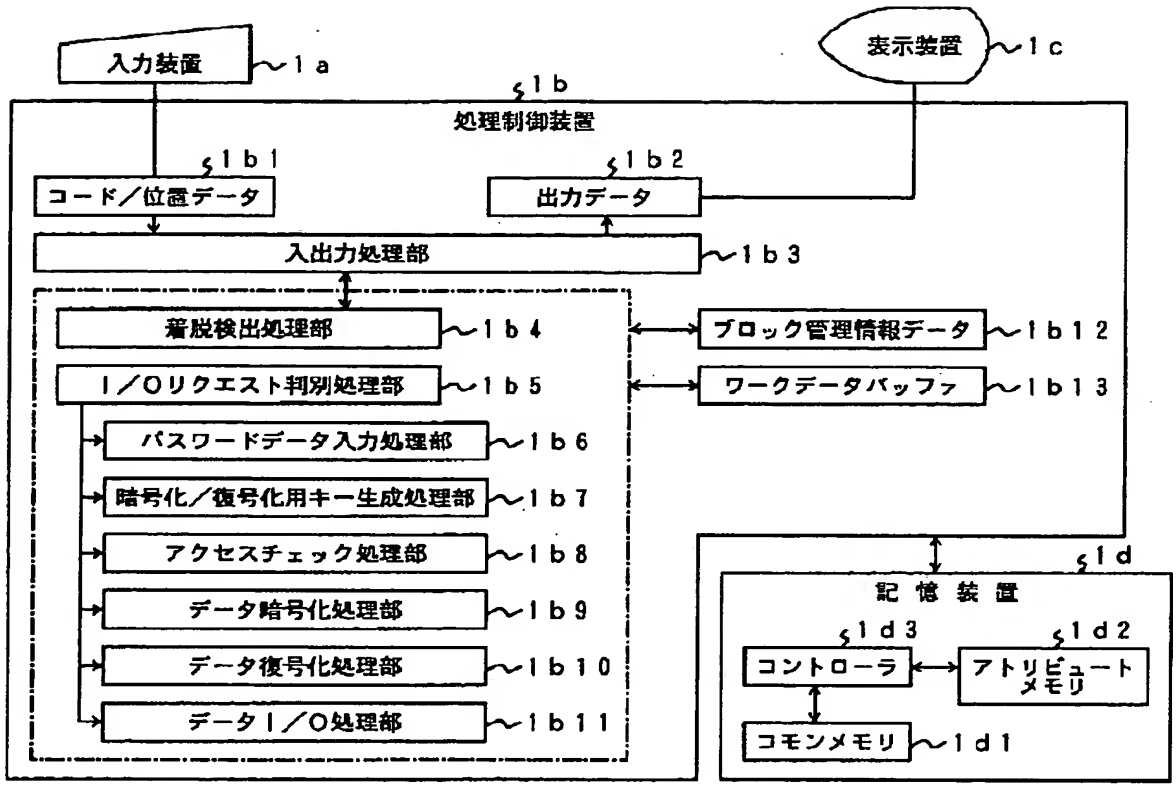
【図５】同実施形態の計算機システムにおけるカード認識処理の流れを説明するフローチャート。

【図６】図５のカード認識処理を行った場合におけるＩ／Ｏ処理の流れを説明するフローチャート。

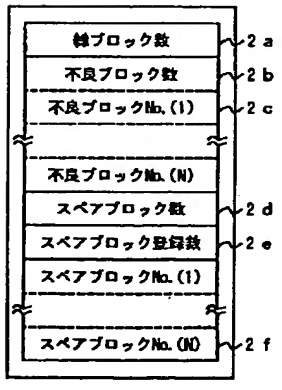
【符号の説明】

１ｂ…処理制御装置、１ｄ…ＰＣカード、１ｂ４…着脱検出処理部、１ｂ５…Ｉ／Ｏリクエスト判別処理部、１ｂ６…パスワードデータ入力部、１ｂ７…暗号化／復号化用キー生成処理部、１ｂ８…アクセスチェック処理部、１ｂ９…データ暗号化処理部、１ｂ１０…データ復号化処理部、１ｂ１１…データＩ／Ｏ処理部。

【図１】

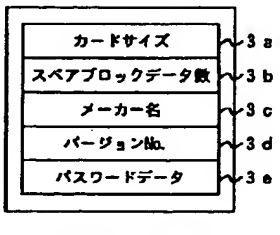


【図２】



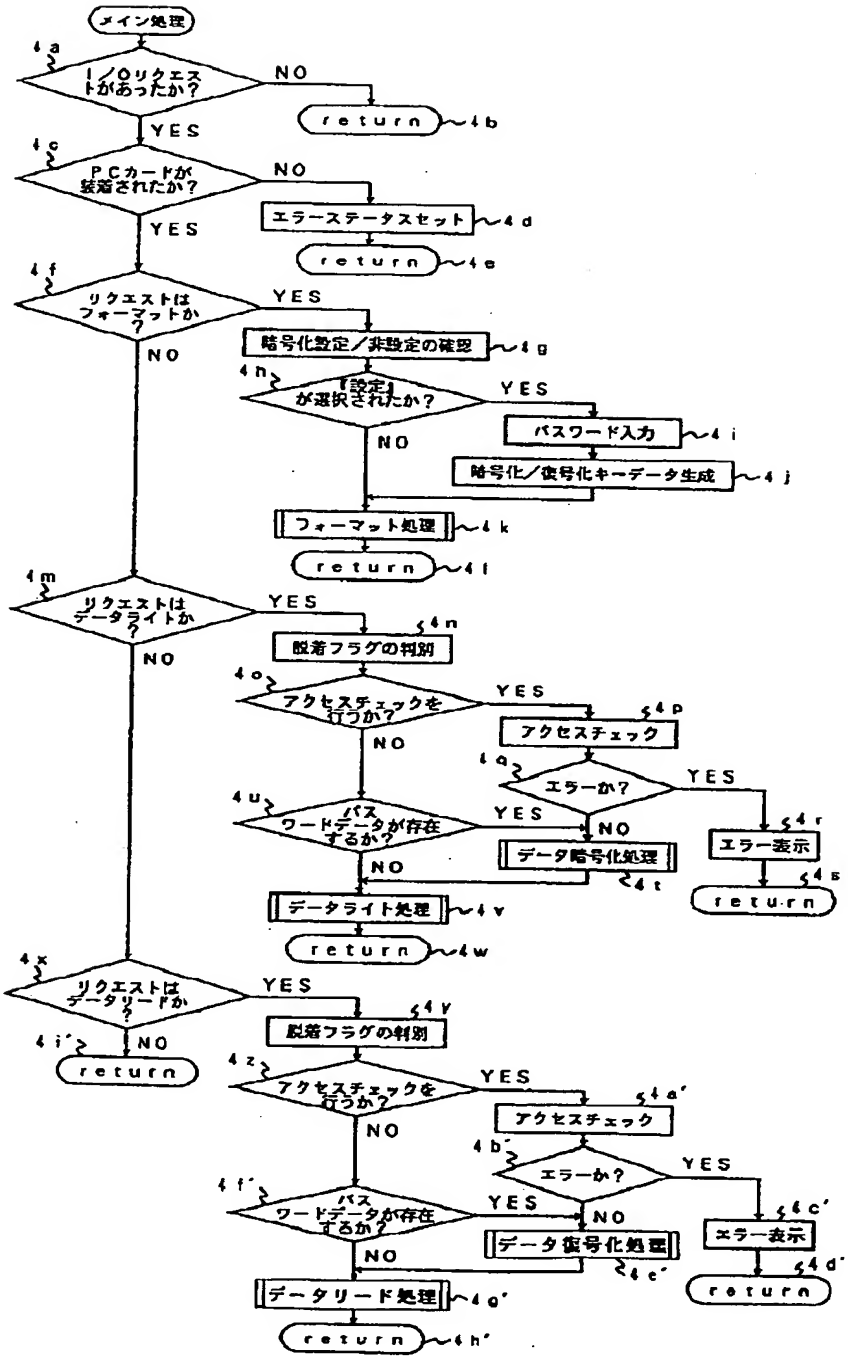
ブロック管理情報データ

【図３】

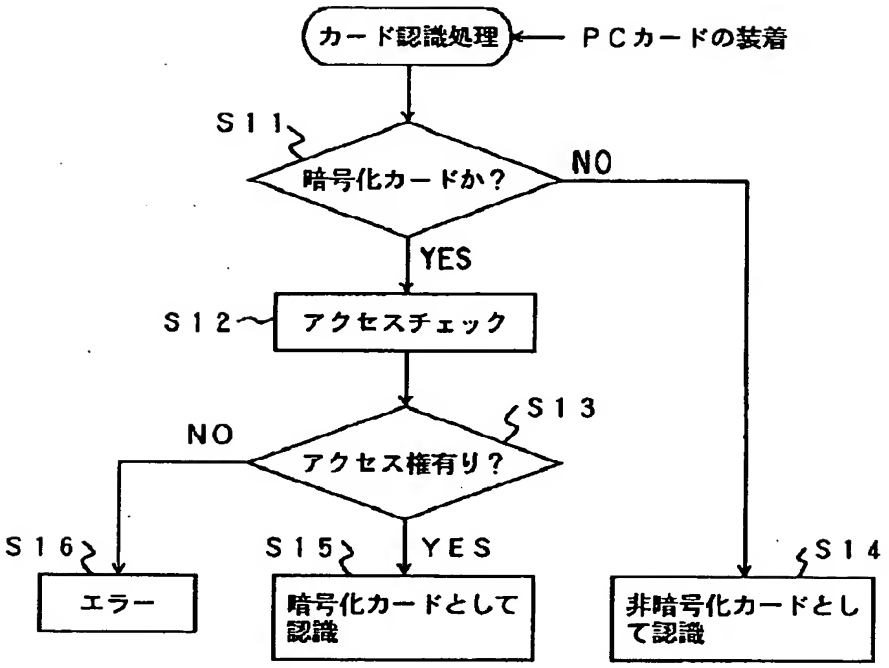


アトリビュートメモリ

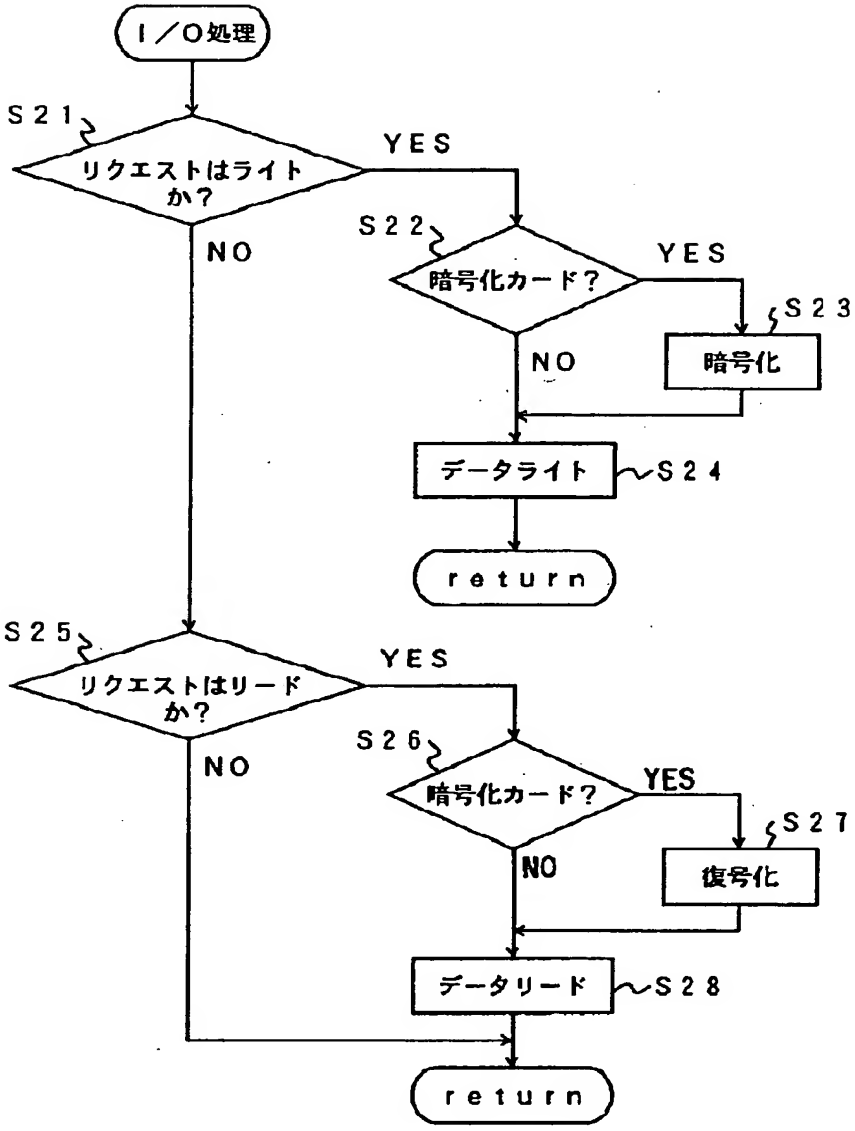
【図４】



【図５】



【図６】



フロントページの続き

(51)Int.Cl.⁶		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｚ	
	9/32					６７３Ａ	